Belden

Cyber Resilience Act: von der Anforderung zur Umsetzung

Was Hersteller, Betreiber und Asset Owner wissen müssen

White Paper

Von **Nils Buecker, Loic Caseras, Tobias Heer** und **André Lehmann** | Belden

Management summary

Digitale Produkte spielen eine zentrale Rolle in Industriebetrieben, Infrastruktursystemen und im Alltag. Mit zunehmender Vernetzung sind diese Geräte – zusammen mit den Softwareplattformen, die sie unterstützen – zu attraktiven Zielen für Cyberangriffe geworden.

Ursprünglich wurden viele dieser vernetzten Produkte mit Hauptaugenmerk auf schnelle Markteinführung und neue Funktionalitäten entwickelt, während Cybersicherheitspraktiken sich langsamer entwickelten, obwohl **Angriffe zunehmend gezielt auf sie ausgerichtet sind.**

Bestehende Gesetze, wie die Network and Information System 2 (NIS2)-Richtlinie, die Critical Entities Resilience (CER)-Richtlinie und verschiedene sektorspezifische Richtlinien, haben versucht, die Cybersicherheitsstandards zu erhöhen und die Verantwortlichkeiten angesichts der drohenden Angriffe zu klären. Aber die Gesetze haben auch ein uneinheitliches System an Vorgaben geschaffen, das je nach Land und Produkttyp unterschiedlich ist. Dadurch sind die Anforderungen schwer zu interpretieren und die Einhaltung der Vorgaben schwer zu verstehen.

Angesichts des aktuellen Stands der digitalen Abhängigkeit ist eine übergreifende Regulierung, die einen Mindeststandard für eingebaute Cybersicherheit in allen Produkten mit digitalen Elementen schafft, von entscheidender Bedeutung. Dies gilt insbesondere für industrielle Netzwerktechnik- und OT-Umgebungen, wo die Sicherheit aufgrund langer Lebenszyklen, veralteter Systeme und komplexer Lieferketten hinterherhinkt.

Die Europäische Union (EU) hat im Jahr 2024 den Cyber Resilience Act (CRA) eingeführt, um **zielorientierte, technologieneutrale Cybersicherheitsanforderungen für Verbraucher- und Industrieprodukte festzulegen.** Diese Anforderungen machen Erwartungen verständlicher, einheitlicher und transparenter.

Die CRA ersetzt weder NIS2 noch andere nationale und internationale sektorale Vorschriften. Stattdessen fungiert sie als Ergänzung.

Dieser Leitfaden hilft Ihnen zu verstehen, was die CRA ist, warum sie wichtig ist und welche Schritte Sie unternehmen sollten, um auf die Änderungen in Produktdesign, Dokumentation und Lebenszyklusunterstützung vorbereitet zu sein.

Inhaltsverzeichnis

Was Sie über den Cyber Resilience Act wissen müssen

Die Kernelemente des Cyber Resilience Act sind für Sie – egal ob Hersteller, Betreiber oder Asset-Besitzer – von entscheidender Bedeutung, um sichere, konforme Industriesysteme zu entwickeln, einzusetzen und zu warten.

Was ist CRA?

Der Cyber Resilience Act ist eine EU-Verordnung, die verbindliche Cybersicherheitsanforderungen für alle Hardware- und Softwareprodukte mit digitalen Elementen einführt. Dies umfasst auch Industrieprodukte, die häufig Hardware, Firmware und Software miteinander kombinieren (einschließlich Cloud-Verbindungstechnik und Fernverwaltung). **Die CRA-Anforderungen gelten für den gesamten Lebenszyklus des Produkts, von der Entwicklung bis zum Ende des Supports.**

Da diese Geräte im Kern kritischer Infrastrukturnetze eingesetzt werden, führt eine stärkere Absicherung der Geräte auch zu einer höheren Sicherheit der verbundenen Netzwerke.

Durch die Festlegung einheitlicher, sektorübergreifender Regeln für Produkte mit digitalen Elementen stellt die CRA sicher, dass Sicherheit nicht nur nachträglich bedacht wird, sondern ein integraler Bestandteil der Planung, Entwicklung und Wartung von Produkten mit digitalen Elementen ist.

Wenn Hersteller ein Produkt auf dem EU-Markt verkaufen möchten – oder wenn Betreiber und Asset-Besitzer dieses Produkt für den Einsatz in einer EU-Umgebung erwerben möchten – muss das Produkt die wesentlichen Cybersicherheitsanforderungen gemäß CRA erfüllen. Andernfalls ist der Verkauf der Produkte nicht zulässig.

Wen betrifft die CRA?

Die Verordnung gilt für Hersteller, die Produkte mit digitalen Elementen für den EU-Markt herstellen, einschließlich Hersteller von Geräten der industriellen Netzwerktechnik, Automatisierungsgeräten und zugehöriger Software. Es sind auch Originalgerätehersteller (OEMs) eingeschlossen, die Geräte für Industrielle Automatisierung und Steuerungssysteme herstellen.

CRA gilt unabhängig davon, wo Hersteller lokalisiert sind. Anbieter außerhalb der EU, die Produkte in den EU-Markt liefern, müssen die CRA-Anforderungen entweder über den Importeur oder direkt erfüllen, indem sie zentrale Pflichten wie die folgenden wahrnehmen:

- Durchführung einer Risikobewertung
- Implementierung und Dokumentation sicherer Entwicklungspraktiken
- Implementierung strukturierter Schwachstellenmanagement-Prozesse
- Unterstützung des Lebenszyklus
- Erfüllung aller zusätzlich anwendbaren CRA-Anforderungen

Für Hersteller mit Sitz in der EU, die ihre Produkte auf dem EU-Markt in Verkehr bringen, gelten die gleichen Verpflichtungen.

Für Hersteller, die bisher keinen Schwerpunkt auf Cybersicherheit gelegt haben, können diese Anforderungen bedeutende Veränderungen notwendig machen. Für Unternehmen, die bereits Frameworks zur Unterstützung sicherer Entwicklungsprozesse eingeführt haben, sind die erforderlichen Änderungen oft besser zu bewältigen und können durch die Erweiterung bestehender Prozesse adressiert werden.

Auch Betreiber und Anlagenbesitzer sind betroffen: Sie werden bei der Planung, dem Kauf und dem Betrieb ihrer Systeme zunehmend CRA-konforme Produkte benötigen, um regulatorische und Sicherheitsverpflichtungen zu unterstützen.

Welche Produkte sind betroffen?

CRA umfasst Produkte, die Software oder digitale Logik enthalten. Diese Liste ist nicht vollständig, umfasst aber unter anderem folgende Produkte:

- Firewalls und Intrusionerkennungs-/präventionssysteme
- Router, Modems und Switches
- Netzwerkmanagementsysteme
- Betriebssysteme

Die Verordnung konzentriert sich nicht auf die Zulassung von „Produktfamilie“, sondern gilt für jede in Verkehr gebrachte Einheit. Jeder ausgelieferte Switch, Router oder Software-Download muss die Anforderungen zum Zeitpunkt des Inverkehrbringens auf dem EU-Markt erfüllen. Die Produktklassifizierung bestimmt den Typ der erforderlichen Zulassung.

Darüber hinaus erwartet die CRA von den Herstellern, dass sie Sicherheitslücken in ihrem eigenen Code sowie in Drittanbieterbibliotheken und Komponenten (Open-Source-Stacks, Verschlüsselungsbibliotheken, Parser oder Hersteller-SDKs) für die Dauer des veröffentlichten Supportzeitraums verwalten. Andernfalls können Schwachstellen in diesen Komponenten dazu führen, dass ein gesamtes Produkt nicht konform ist.

Wie wird die Einhaltung der CRA-Vorschriften überprüft?

Zur Durchsetzung der CRA-Regeln werden nationale Marktüberwachungsbehörden in jedem Mitgliedstaat die Einhaltung über verschiedene Kanäle überwachen.

- Berichte aus der eigenen Organisation eines Herstellers
- Eigene Untersuchungen und Marktscreenings
- Berichte aus anderen Quellen

Die CRA integriert ihre Anforderungen auch in das CE-Kennzeichnungssystem. Das CE-Zeichen signalisiert nun, dass ein Produkt nicht nur die Anforderungen an Sicherheit und elektromagnetische Verträglichkeit (EMV) erfüllt, sondern auch die Cybersicherheitsanforderungen der CRA. Bevor sie das CE-Zeichen anbringen dürfen, müssen Hersteller Konformitätsbewertungen gemäß CRA und die erforderliche technische Dokumentation abschließen. Importeure und Distributoren müssen sicherstellen, dass nur CRA-konforme und CE-gekennzeichnete Produkte auf den EU-Markt gelangen.

CRA und NIS2: Wie die Vorschriften zusammenhängen

Da die Cybersicherheitsvorschriften in ganz Europa immer strenger werden, arbeiten CRA und NIS2 zusammen, wobei sich CRA darauf konzentriert, wie Produkte gebaut werden, und NIS2 darauf, wie Produkte eingesetzt und betrieben werden.

Betreiber, die dem NIS2 unterliegen, werden zunehmend CRA-fähige Produkte fordern, um ihren eigenen Verpflichtungen nachzukommen. Der Einsatz von Geräten, die nicht den Anforderungen der CRA entsprechen, könnte die Sicherheit und die Einhaltung gesetzlicher Vorschriften gefährden.

Die CRA wird die Beschaffungskriterien beeinflussen, wobei Betreiber zunehmend von Anbietern verlangen, CRA-konforme Entwicklungsprozesse, Schwachstellenmanagement und Lebenszyklus-unterstützung nachzuweisen.

Gemeinsam treiben CRA und NIS2 die Cybersicherheit tiefer in die Lieferkette hinein: Hersteller müssen sichere Produkte entwickeln, und Betreiber müssen diese Produkte im Rahmen eines risikobasierten Sicherheitsprogramms auswählen und verwalten.

Dies wird eine engere Zusammenarbeit zwischen OEMs und Betreibern bei Themen wie SBOM-Transparenz, Update-Strategien und Vorfallkommunikation bedeuten.

5 entscheidende CRA-Anforderungen zum Verständnis

Die CRA legt zentrale Anforderungen fest, um Hersteller bei der Entwicklung, dem Bau und der Wartung sicherer Produkte mit digitalen Elementen zu unterstützen. Sie geben Betreibern und Asset-Besitzern zudem klare Zusicherungen bezüglich des Sicherheitsniveaus der von ihnen eingesetzten Geräte.

1. Sicherheit durch Design und Voreinstellung

Produkte sollten entworfen, entwickelt und produziert werden, um ein angemessenes Maß an Cybersicherheit sicherzustellen. Sie müssen mit sicheren Voreinstellungen, Konfigurationen und Schutzmaßnahmen ausgeliefert werden, die unsichere Konfigurationen unwahrscheinlicher machen und typische Angriffswege minimieren.

Grundlegende Schutzmaßnahmen wie robuste Authentifizierung, kryptografische Anforderungen, Schlüssellängen, zugelassene Algorithmen, obligatorische Sicherheitskontrollen, verschlüsselte Kommunikation und gehärtete Standardeinstellungen werden in vielen Fällen als Basiserwartungen gelten.

Insgesamt gilt jedoch ein risikobasierter Ansatz: Sicherheitsmaßnahmen sollten **die aktuellen Best Practices und den Stand der Technik für das Produkt widerspiegeln.** Zum Beispiel sollten Hochrisikoprodukte strenge und umfassende Kontrollen implementieren, während bei Produkten mit geringerem Risiko ein weniger strenger Maßnahmenkatalog ausreichen kann. Dies bedeutet auch, sich auf neue Bedrohungen durch Planung und Überwachung kryptografischer Leitlinien vorzubereiten und einen Übergang zu quantenresistenten Algorithmen zu planen, sobald diese ausgereift und standardisiert sind.

2. Sicherer Entwicklungslebenszyklus

Hersteller müssen einen strukturierten, sicheren Entwicklungslebenszyklus implementieren, der Folgendes umfasst:

- Bedrohungs- und Risikoanalysen mithilfe eines strukturierten Bedrohungsmodellierungsverfahrens
- Sichere Programmierpraktiken
- Prüfung und Verifizierung
- Dokumentation von Sicherheitsentscheidungen

Die Anpassung des Entwicklungsprozesses an Standards wie IEC 62443-4-1 kann Herstellern helfen, diese Erwartung zu erfüllen und Nachweise für Praktiken im sicheren Entwicklungslebenszyklus zu erbringen. Der Standard stellt eine definierte Reihe von Aktivitäten, Dokumenten und Kontrollpunkten bereit, die Prüfern, Betreibern oder Asset-Eigentümern als Nachweis vorgelegt werden können, dass Sicherheit während der gesamten Entwicklung systematisch berücksichtigt wurde.

3. Schwachstellenvorfälle, Bearbeitung und Offenlegung

Hersteller müssen Schwachstellen während des gesamten Produktlebenszyklus überwachen, identifizieren und beheben, einschließlich der Erkennung und Berichterstattung aktiv ausgenutzter Schwachstellen und schwerwiegender Vorfälle an die Behörden innerhalb festgelegter Fristen. Dieser Prozess sollte einer dokumentierten Richtlinie für die Reaktion auf Sicherheitsvorfälle folgen, die Schweregrade, Reaktionsziele und Eskalationswege definiert.

Hersteller müssen außerdem Prozesse einrichten, um Schwachstellenberichte zu erhalten, mit Betreibern und Asset-Besitzern zu kommunizieren und unverzüglich Aktualisierungen bereitzustellen, sobald Probleme entdeckt werden. Kritische Schwachstellen (definiert anhand einer standardisierten Bewertungsmethode wie dem Common Vulnerability Scoring System, CVSS) sollten eine schnelle Bewertung und eine erste Benachrichtigung der Betreiber oder Anlagenbesitzer innerhalb vereinbarter Service-Level-Ziele auslösen, gefolgt von regelmäßigen Statusupdates und einer zeitnahen Bereitstellung von Sicherheitsupdates.

4. Lebenszyklus-Support und Updates

Hersteller müssen den definierten Unterstützungszeitraum klar kommunizieren, damit Benutzer, Betreiber und Asset-Besitzer wissen, **wie lange das Produkt Sicherheitsupdates erhält** und was „unterstützt“ tatsächlich bedeutet.

Sicherheitsupdates müssen dann vom Produktstart bis zum angekündigten Supportende bereitgestellt werden, zusammen mit klaren Informationen darüber, wie Updates ausgeliefert und angewendet werden.

5. Technische Dokumentation und Benutzerinformationen

Die technische Dokumentation dient als interne und behördliche Nachweisgrundlage, um zu zeigen, **wie ein Produkt die Anforderungen des Cyber Resilience Act (CRA) erfüllt** und wie die Sicherheit über seinen gesamten Lebenszyklus hinweg verwaltet wird. Die für die Konformität erforderliche interne Dokumentation sollte Folgendes umfassen:

- Risikobewertungen
- Cybersicherheitsmerkmale
- Entwicklungs- und Testaktivitäten
- Schwachstellenverwaltungsprozesse

Wenn diese technischen Dokumente extern geteilt werden, sollten sie darlegen, was Betreiber und Asset-Besitzer wissen müssen, um das Produkt sicher zu implementieren und zu betreiben, einschließlich folgender Produkteigenschaften:

- Cybersicherheitsmerkmale
- Aktualisierungsmechanismen
- Supportzeitraum
- Anforderungen an eine sichere Konfiguration
- Verantwortlichkeiten der Benutzer für die Aufrechterhaltung der Sicherheit

Technische Dokumentation und Konformitätserklärungen sind aufzubewahren, damit die Behörden die fortlaufende Einhaltung überprüfen können.

Die nächsten Schritte auf dem Weg zur CRA-Konformität

Um für die CRA gerüstet zu sein, ist es an der Zeit für Hersteller, Betreiber und Asset-Besitzer, Prozesse zu formalisieren, Verantwortlichkeiten zu klären und die Zusammenarbeit entlang der Lieferkette zu intensivieren.

Um die Einhaltung der Vorschriften zu vereinfachen, wählen Sie Partner mit ausgewiesener Expertise im Bereich industrieller Cybersicherheit, beispielsweise IEC 62443-zertifizierte Entwicklungsprozesse und etablierte Prozesse für das Schwachstellenmanagement. Auf diese Weise wird ein Teil der aufwändigen Arbeit im Zusammenhang mit sicherer Entwicklung und der Generierung von Nachweisen bereits auf Anbieterseite erledigt sein.

Nächste Schritte für Hersteller von Industrieprodukten

Bevor Sie Produkte auf dem EU-Markt in Verkehr bringen, müssen industrielle Produkthersteller bereit sein, Folgendes zu tun:

- Führen Sie eine Konformitätsbewertung durch und bereiten Sie eine EU-Konformitätserklärung vor, die die Cybersicherheit abdeckt. Die technische Dokumentation ist mindestens fünf Jahre oder während des Supportzeitraums aufzubewahren.
- Dokumentieren Sie klare Supportzeiträume sowie Aktualisierungsrichtlinien und Entscheidungen zum Supportende, um Überraschungen zu vermeiden und Betreibern sowie Asset-Besitzern bei der Planung von Lebenszyklusstrategien zu helfen.
- Entwickeln Sie eine Strategie für Software-Stücklisten (SBOMs), Governance von Drittanbieterkomponenten und koordiniertes Schwachstellenmanagement über den gesamten Stack hinweg, einschließlich der Verwendung eines standardisierten SBOM-Formats wie SPDX oder CycloneDX.
- Vergleichen Sie die aktuellen Entwicklungspraktiken mit den CRA-Anforderungen und Rahmenwerken, wie beispielsweise IEC 62443-4-1 und IEC 62443-4-2, um Lücken in sicherem Design, Test, Dokumentation und Schwachstellenmanagement zu identifizieren.
- Etablieren oder verfeinern Sie sichere Entwicklungslebenszyklen, SBOM-Generierung, Verwaltung von Drittanbieterkomponenten und Richtlinien zur Lebenszyklusunterstützung, damit diese in einer CRA-Konformitätsbewertung nachgewiesen werden können.

Nächste Schritte für Betreiber und Asset-Besitzer

- Um sich auf die Auswirkungen der CRA auf die Lieferkette vorzubereiten, sollten Betreiber und Asset-Besitzer die folgenden Schritte unternehmen:
- Erfassen Sie kritische Systeme, die auf Produkten mit digitalen Elementen basieren, und identifizieren Sie, wo CRA-ready-Produkte bereits im Rahmen von Modernisierungsmaßnahmen eingesetzt werden oder deren Einsatz geplant ist.
- Stellen Sie den Lieferanten Fragen dazu, wie sie mit Sicherheitslücken umgehen, wie lange Produkte Sicherheitsupdates erhalten, wie Drittanbieterkomponenten verwaltet werden, wie sie sich auf die Fristen der CRA vorbereiten, ob sie SBOMs in einem anerkannten Format bereitstellen können usw.

Warum alle Hersteller frühzeitig handeln müssen

Produkte mit bekannten, ausnutzbaren Sicherheitslücken dürfen nicht auf den Markt gebracht werden. In diesem Fall können die Behörden Korrekturmaßnahmen, Rückrufe oder die Rücknahme von Produkten anordnen.

Frühe Vorbereitung verringert das Risiko von Verzögerungen bei der Markteinführung, erzwungenen Neugestaltungen in letzter Minute und der Möglichkeit, dass Produkte nicht auf den EU-Märkten verkauft werden können.

Neue Produkte, die nach dem Anwendungsdatum auf dem EU-Markt in Verkehr gebracht werden, müssen alle Anforderungen erfüllen. Zusätzliche Fristen gelten beispielsweise für die Berichterstattung und dafür, wie lange bestehende Produkte verfügbar bleiben dürfen.

Wenn Hersteller bis kurz vor Ablauf dieser Fristen warten, riskieren sie blockierte Produkteinführungen, hastige Änderungen und gegebenenfalls Sanktionen, wenn die Verpflichtungen nicht rechtzeitig erfüllt werden.

IEC 62443 als Grundlage für CRA

IEC 62443 ist weithin anerkannt als Referenzstandard für die Sicherung industrieller Automatisierungs- und Steuerungssysteme und kann Herstellern dabei helfen, Nachweise und Dokumentation zur Unterstützung von CRA-Konformitätsbewertungen zu generieren. Unternehmen, die dieser Norm folgen, sind in einer starken Position, sich an die CRA-Vorschriften anzupassen.

CRA steht im Einklang mit:

- **IEC 62443-4-1,** die einen sicheren Produktentwicklungslebenszyklus definiert, der die Lebenszyklusverpflichtungen des CRA unterstützt.
- **IEC 62443-4-2,** die technische Sicherheitsanforderungen für Komponenten definiert, um den CRA-Anforderungen an „secure-by-design“ und „secure-by-default“ Produkte gerecht zu werden.
- **IEC 62443-3-3,** wobei der Fokus auf der Sicherheit auf Systemebene liegt, damit Betreiber sichere Komponenten in sichere industrielle Netzwerke integrieren können.

Es ist außerdem wichtig, die Grenzen der Ausrichtung zu erkennen. Die CRA führt zusätzliche rechtliche und administrative Anforderungen ein, wie Vorfallmeldungen, CE-Markierungsprozesse, Bekanntgabe von Support-Dauern und Aufbewahrungsfristen für Dokumentation, die von IEC 62443 nicht abgedeckt werden. Hersteller müssen die regulatorischen Anforderungen der CRA zusätzlich zur IEC 62443 umsetzen.

Wie Belden CRA-konforme Produktsicherheit unterstützt

Als Hersteller mit einem Ruf für den Schwerpunkt auf Sicherheit während der Produktentwicklung liefert Belden sichere industrielle Netzwerkprodukte und langfristige Unterstützung im Produktlebenszyklus, sodass diese sicher in Ihre Sicherheitsprogramme integriert werden können.

Dies erreichen wir durch einen zertifizierten Secure Produkt Development Lifecycle, global harmonisierte Prozesse und eine starke Sicherheits-Governance, die Ihnen helfen, die Erwartungen der CRA über den gesamten Produktlebenszyklus hinweg zu erfüllen.

Sichere Produktentwicklung

Um Sicherheit in jede Phase der Produktentwicklung einzubinden, betreibt Belden einen **Sicheren Produkt-entwicklungslebenszyklus** über sein Portfolio der industriellen Netzwerktechnik hinweg, der an IEC 62443-4-1 ausgerichtet ist. Es umfasst sicheres Design, Implementierung, Verifizierung und Wartung, einschließlich strukturierter Bedrohungsmodellierung, Angriffsflächenanalyse und Risikobewertungen basierend auf standardisierten Methoden wie den STRIDE- oder PASTA-Frameworks. Sicherheit wird als wiederholbarer ingenieurtechnischer Prozess behandelt, nicht als einmalige Konzentration auf einzelne Produkte.

Stand März 2026 **verfügt Belden über eine globale IEC 62443-4-1-Zertifizierung mit Reifegrad 4,** was eine unabhängige Bestätigung unserer sicheren Entwicklungspraktiken bietet.

Globale Praktiken über den gesamten Lebenszyklus hinweg

Um eine konsistente Sicherheitserfahrung über Produkte und Regionen hinweg zu gewährleisten, begann Belden im Jahr 2023 damit, seine ausgereifteste, auf IEC 62443-4-1 basierende Entwicklungsumgebung als gemeinsamen Standard für alle F&E-Standorte weltweit einzuführen.

Neue Produkte werden **auf Basis einer einheitlichen Sicherheits-Baseline** und einer langfristigen Lifecycle-Unterstützungsstrategie entwickelt, unabhängig davon, wo sie konstruiert, entworfen oder hergestellt werden.

Verbindungen zu übergeordneten Standards und Governance

Über die Produktentwicklung hinaus richtet Belden seine Produktsicherheitsarbeit an umfassenderen Informationssicherheitsstandards wie IEC 62443 und ISO 27001 aus. Hersteller, Betreiber und Asset-Besitzer können darauf vertrauen, dass Geräteschutz durch **organisatorische Kontrollen in Bezug auf Daten, Prozesse und die Reaktion auf Sicherheitsvorfälle verstärkt wird.**

Die interne Governance umfasst zentrale Sicherheitsbüros und Beratungsfunktionen, die die Einhaltung des Secure Produkt Development Lifecycle überwachen und CRA-bezogene Aktivitäten koordinieren, sodass regulatorische Erwartungen einheitlich und kohärent verwaltet werden.

Jetzt schon auf die zukünftige Regulierung vorbereiten

CRA wird die Erwartungen an Industrielle Netzwerktechnik und Automatisierungsgeräte neu gestalten. Cybersicherheit wird zu einem unverzichtbaren Merkmal von Produkten mit digitalen Elementen werden.

Wer bereits heute Entwicklungsprozesse, Produktportfolios und Beschaffungsrichtlinien anpasst, **ist besser darauf vorbereitet, Marktzugangsprobleme und kurzfristige, reaktive Änderungen später zu vermeiden.**

Durch die Kombination von IEC 62443-4-1-basierter sicherer Entwicklung, globaler Prozessharmonisierung und einer langfristigen Wartungsmentalität möchte Belden Sie dabei unterstützen, die CRA zu navigieren.

Unsere CRA-fähigen Produkte, kombiniert mit unserer Unterstützung bei der Integration dieser Produkte in sichere, konforme Industriearchitekturen über den gesamten Lebenszyklus, helfen Herstellern**, Compliance-Risiken zu minimieren und ein hohes Sicherheitsniveau aufrechtzuerhalten**, während sich die Anforderungen weiterentwickeln.

Mehr erfahren

Connect to what's possible.

White Paper

Über Belden

Belden Inc. liefert Komplettlösungen für die Verbindungstechnik, die ungeahnte Möglichkeiten für unsere Kunden, deren Kunden und die Welt eröffnen. Wir treiben Ideen und Technologien voran, die eine sicherere, intelligentere und wohlhabendere Zukunft ermöglichen. Im Laufe unserer über 120-jährigen Geschichte haben wir uns als Unternehmen weiterentwickelt, aber unser Ziel bleibt dasselbe – Verbindungen herzustellen. Indem wir Menschen, Informationen und Ideen miteinander verbinden, machen wir es möglich. Unser Hauptsitz befindet sich in St. Louis und wir verfügen über Fertigungskapazitäten in Nordamerika, Europa, Asien und Afrika.

Weitere Informationen finden Sie unter:
belden.com

Folgen Sie uns auf

Belden